TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Raido Pahtma

Traadita sensorvõrgud, ründed ja kaitse

Tallinn 2008

Traadita sensorvõrgud – tark tolm, arupuru

Targa tolmu, kübemete või arupuru all mõistetakse miniatuurseid traadita sidevõimaluse ja autonoomse energiaallikaga arvutusseadmeid, mis on varustatud erinevate sensoritega. Kübemeid saab kasutada keskkonnast informatsiooni hankimiseks ja töötlemiseks. Sidevõimalus ja autonoomne energiaallikas võimaldavad neid rakendada väga erinevates kohtades ja tingimustes – potentsiaalsed kasutusvaldkonnad ulatuvad lihtsalt paigaldatavatest mõõteseadmetest militaarsete jälitus- ja jälgimisvahenditeni.

Praegused masstootmises olevad kübemed kasutavad valdavalt Atmega128 ja sellele parameetritelt sarnaseid mikrokontrollereid ning töötavad kahe AA patareiga. Side jaoks kasutatakse nende kübemete puhul kas 433, 868, 916Mhz või 2.4GHz sagedusel töötavaid raadiomooduleid. Juba seadmete nimetus – tark tolm – viitab aga sellele, et tegemist peaks olema millegi märksa väiksema ja keskkonnas praktiliselt nähtamatuga. Kahjuks eelpool kirjeldatud riistvaraga seadmed aga selliste omadustega ei ole. Olemasoleva tehnoloogiaga ei ole paljude vajalike komponentide mõõtmete kahandamine ja ühele kristallile integreerimine tegelikult probleemiks ning olemas on ka vaid mõne kuupmillimeetrise ruumalaga prototüübid[3]. Paraku üheks suurimaks takistuseks on piisavalt kompaktsete, pika elueaga ja mõistliku hinnaga kübemete tootmisel sobivate energiaallikate puudumine. Palju arenguruumi on veel ka kommunikatsioonilahendustel. Nende puuduste likvideerimise kallal töötavad aga paljud ettevõtted üle maailma ning lootustandvaid tehnoloogiaid on mitmeid, näiteks seadmed, mis toodavad elektrienergiat vibratsioonist, elektromagnetkiirgusest või radioaktiivsete materjalide lagunemisest. Taolised kauakestvad või taastuvad energiaallikad võimaldavad kübemetele anda väga pika, teoreetiliselt sadade aastate pikkuse eluea. Siiski tuleb eeldada seda, et ka kõige paremate miniatuursete energiaallikate võimsus jääb alla selle, mida seadmed ise on võimelised tarbima ning arvutusi ja kommunikatsiooni tuleb optimeerida just energia seisukohast.

Sensorvõrkude rakendused

Sensorvõrkude, nagu paljude teiste uute tehnoloogiate, kasutamise vastu on suurt huvi üles näidanud erinevate riikide sõjaväed. Miniatuursetele ja autonoomsetel sensoritel on mitmeid erinevaid kasutusvõimalusi valvatavatel aladel, olgu siis tegemist aktiivse lahinguväljaga või turvatava linnaosaga. Kübemed pakuvad erinevaid võimalusi informatsiooni kogumiseks, sealhulgas vaenlase sõdurite ja sõidukite avastamiseks või snaiperite leidmiseks. Sensorandmete analüüs võimaldab efektiivselt eristada sõbralikke ja vaenulikke üksuseid ning koordineerida

ressursside jaotamist. Sensorvõrkude ja mehitamata lennumasinatega on võimalik luua efektiivsem ja turvalisem alternatiiv konfliktijärgsel rahuajal tarbetult elusid nõudvatele miiniväljadele.

Targa tolmu rakendused ei piirdu aga kindlasti ainult militaarsektoriga ning omavad tulevikus kindlat kohta nii tervishoius, kaubanduses kui ka ehituses, võimaldades realiseerida kõikjal oleva arvutuse(ubiquitous computing) ideesid. Kübemeid sobivalt riietesse, võib-olla aga ka naha alla või mujale organismi integreerides on võimalik tagada pidev inimese tervisliku seisundi jälgimine ning kübemetega saaks lihtsustada ja efektiivsemaks muuta mitmeid meditsiiniuuringuid.

RFID hinnalipikute ja tähiste kasutamisest on palju räägitud ja need võimaldavad kaupade ning esemete liikumist ja arvepidamist märkimisväärselt lihtsustada, kübemed aga võimaldavad palju rohkemat. Erinevalt RFID märkidest saab soovitud eset otsida kübemevõrgu kaudu ilma konkreetse eseme lähedusse minemiseta, veelgi enam, saades teada, et soovitud omadustega kaup on näiteks laos olemas, võivad kübemed leviraadiuse põhise positsioneerimise[4] abil välja selgitada selle asukoha.

Sobivate anduritega varustatud kübe võimaldab meil jälgida toote olukorda transpordi ja töö ajal ning ennustada ja diagnoosida võimalikke rikkeid või muutusi tootele mõju avaldanud keskkonnaomadustest lähtuvalt. Külmkapp võiks näiteks teada, et hoiustatavas piimapakis olev piim hakkab tõenäoliselt hapuks minema, kuna pakk seisis liiga kaua soojas toas. Samuti saaks varguste vastu ilmselt üpriski efektiivselt võidelda, kui esemed tunneksid oma omanikku ja oleksid võimelised märku andma loata teisaldamise katsetest.

Paigaldades arupuru ehitiste ja ja muude suurte konstruktsioonide detailide sisse või külge, saab palju täpsemalt ja väiksemate kulutustega teostada hooldustöid ning tõenäoliselt ennetada paljusid ohtlikke olukordi. Vibratsiooniandurite toestustaladelt saadava informatsiooni alusel võib ära hoida ohtlikke varinguid ning insenerid saaksid hinnata millist mõju on kübemeid sisaldavast betoonist valatud sillale omanud aastakümnete pikkune kokkupuude soolase mereveega.

Esile sai toodud vaid osa potentsiaalsetest targa tolmu rakendustest, kuid ometigi on lihtne mõista, et kõigi nende rakenduste juures on vaja suurt tähelepanu pöörata turvalisusele. Ilma sobivate turvameetmeteta ja käideldavust tõstvate lahendusteta ei saa olla kindel saadava informatsiooni vastavuses tegelikkusele ja võimatu on tagada süsteemide toimimist ühiskondlikult keerulistes oludes. Targa tolmu võrkude spontaanne tööpõhimõte annab sellistele süsteemidele palju võimalusi,

kuid samas tekitab fikseeritud infrastruktuuri puudumine ka mitmeid ohtusid.

Kommunikatsioon sensorvõrgus

Sensorvõrkude põhiideoloogiaks on füüsilise ja fikseeritud võrguinfrastruktuuri puudumine, andmeedastusteede tekkimine spontaanselt ning võimalikult konservatiivne energiakasutus sõnumite saatmisel. Kuna informatsiooni edastamine otse üle pika vahemaa ei ole praktikas kuigi edukalt teostatav, eriti piiratud energiaressursside korral, siis tuleb adressaadini jõudmiseks kasutada teiste võrguliikmete abi(multi-hop). Ilmselgelt ei ole mõistlik lihtsalt kõigi sõnumite kõigile edasi saatmine ja sellega energia raiskamine ning võrgu ummistamine, vaid paigas peavad olema marsruudid. Optimaalse tee leidmine aga on omajagu keeruline ülesanne, juba siis, kui sõlmede paiknemine on teada ja nad on omavahel ühendatud kaablitega. See ülesanne võib esmapilgul tunduda aga lausa võimatuna tingimustes, kus ühendust soovivad seadmed on täiesti juhuslikult heidetud praktiliselt tundmatusse kohta. Seejuures tuleb silmas pidada seda, et optimaalsus on sõltuv olukorrast ning olukord muutub kohtades, kuhu kõige rohkem oleks kübemeid vaja paigutada, väga tihti ja tavaliselt üsnagi ootamatult. Seega tegelikult ei olegi niivõrd tähtis selle kõige parema võrgu ülesehituse leidmine, kuivõrd kiire kohanemisvõime omamine. Siiski ei ole raske mõista, et äärmiselt kasulik on umbkaudne ettekujutus sellest, kus kübemed ja kasutusel olevat kommunikatsioonilahendust mõjutavad objektid keskkonnas paiknevad. See lihtsustab esmast iseorganiseerumist ja ka hilisemat võrgu reaktsiooni muudatustele – paranemisvõimet. Õnneks võimaldavad kübemete andurid ja sidelahendused seda ettekujutust luua. Algoritmid, mis võtavad automaatselt arvesse keskkonda ning kannavad hoolt kübemevõrkude iseorganiseerumise ja võrguliikluse marsruutimise eest on suhteliselt keerulised ja paljuski tegelikult esimestes arengufaasides.

Juba eelnevalt välja toodud ja praegu põhiliselt kasutatavate raadiomoodulite kasuks räägib raadiosignaali võime levida kõigis suundades ning läbi osade füüsiliste objektide. Paraku valmistab tihti probleeme ühine eeter, mille ummistamine võib tavapäraste raadiomoodulite puhul väga kergelt juhtuda ka täiesti legaalse liikluse tõttu, rääkimata siis sihilikust segamisest. Suuremat kiirust, töökindlust ja energiaefektiivsust lubavad ultra-lairiba raadiod, mida aga praegu on kübemete peal veel vähe katsetatud. Raadio kasutamisel on lisaks veel selline ebameeldiv omadus, et eetri kuulamine võtab üpris palju energiat, tihti rohkem kui sõnumite saatmine. See aga tähendab, et kübe peab võimalikult palju ajast hoidma raadiot väljalülitatuna ning sõnumi algus võib märkamatuks jääda. Seega muutub oluliselt raskemaks sõnumite edastamise – kohalejõudmata

sõnum võidakse küll uuesti saata, kuid see koormab võrku, kulutab energiat ja tekitab viite. Raadio puhul ei saa ka kuidagi vältida pealtkuulamise ohtu, raskeks saab ainult teha sõnumitest arusaamise.

Raadio asemel või tõenäoliselt pigem raadiole lisaks võiks aga kasutada sõnumite edastamiseks valgussignaale. Põhimõtteliselt võimaldab olemasolev tehnoloogia luua imepisikesi lasereid ja pööratavaid peegleid[3], mida saab kasutada lasersignaali suunamiseks või püüdmiseks ja andurile peegeldamiseks. Arusaadavalt on tegemist punkt-punkt ühendusega ning seejuures juhuslikult kujunenud võrgus on teise kübeme ülesleidmine ainult laseriga praktiliselt võimatu. Kui aga raadio teel õnnestub teise kübeme orienteeruv asukoht teada saada, siis õnnestub ehk otsenähtavuse korral ka laseri jaoks sobiv seadistus leida. Laseri puhul ei võta erinevalt raadiost signaali vastuvõtmine energiat, vaid tegelikult isegi toodab seda. Samuti on laserühendust ilma füüsilise takistuseta praktiliselt võimatu häirida ja pealt kuulata. Seega kui kübemed varustada korraga nii raadioga kui ka laserside võimalusega, õnnestuks optimeerida teiste kübemetega suhtlemiseks vajalikku energiatarvet ning tekitada üpris turvalisi sidekanaleid.

Sensorvõrkude juures on veel üks oluline aspekt, nimelt ühendus teiste võrkude ja seadmetega. Kuna kübemete näol on tegemist seadmetega, mis eelkõige koguvad informatsiooni keskkonnast, siis on nende tegemistest vähe kasu, kui see informatsioon kasutajateni ei jõua. Tavaliseks lahenduseks on näiteks seadmed, mis on varustatud lisaks kübemete raadiomoodulile ka GSM modemiga. Selle seadme näol on aga ilmselgelt tegemist võimaliku nõrga lüliga kogu süsteemis, kuna kui sellele väravale ei peaks jätkuma toidet, ühendus kübemetega on häiritud või peaks esinema mõni rike, siis jääb võrk muust maailmast eraldatuks. Isegi kui sellises olukorras andmete iseloom võimaldaks hilisemat edastamist, ei ole piiratud mälumahuga kübemed võimelised informatsiooni väga pika perioodi kohta talletama ning üsna tõenäoline on, et midagi vajalikku võib kokkuvõttes kaduma minna. Ühendusseadmeid võib loomulikult võrku panna mitmeid, kuid siiski on tegemist objektidega, mis pigem alluvad tavapäraste mobiilseadmete reeglitele.

Sensorvõrkude turvalisus

Sensorandmete reaalajaline olemus nõuab esiteks kõrget käideldavust, samuti on kontrolli vaja omada informatsiooni saatjate ja vastuvõtjate üle. Internetiliikluse salastamiseks ja autentsuse tagamiseks on välja mõeldud palju teoreetiliselt murtavaid, kuid praktikas reaalsete ja mõistlike vastaste vastu üpriski hästi toimivaid krüptograafialahendusi. Paraku paljud nendest lahendustest ei ole sensorvõrkudes ilma tõsiste muudatuste või ohverdusteta kasutatavad. Mõistliku turvalisuse

taset pakkuvate võtmepikkustega klassikalised avaliku võtme algoritmid(RSA) on kübemete jaoks liiga arvutusmahukad ning ilma nendeta osutub problemaatiliseks arvutuslikult efektiivsema sümmeetrilise krüptograafia võtmevahetus ning kübemete identifitseerimine. Vahetult enne keskkonda paigaldamist kübemetesse laetud ühine salajane võti[1] võib küll mõnda aega hoida liikluse turvalisena, kuid kuna tark tolm paigaldatakse tõenäoliselt kohta, kuhu on võimalik ligi pääseda ka vastasel, siis piisab vaid ühe kübeme ülesleidmisest ja uurimisest, et omandada piiramatu ligipääs kogu võrgule. Avaliku võtme krüptograafia kasutamine ei ole aga kindlasti välistatud, pigem on vaja kasutada efektiivsemaid algoritme[2] koos krüpteerimist teostavate riistvaramoodulitega, mis oleksid kiiremad kontrollerist endast ja tarbiksid seejuures vähem energiat. Alles jääb aga jällegi oht, et kompromiteeritakse mõni konkreetne kübe ja selle salajane võti. Järelikult tuleb suurt tähelepanu pöörata meetoditele, mis võimaldaksid tuvastada vastaste poolt üle võetud kübemeid ning nendega infovahetust vältida.

Sensorvõrgu ründamine ja kaitsmine

Sensorvõrkude rakenduste juures on eelkõige oluline tagada edastatavate andmete korrektsus, võib-olla ka salastatus ning andmete õigeaegne jõudmine nende tarbijateni.

Nagu paljude teiste süsteemide korral on tõenäoliselt kõige vähem teadmisi nõudev võimalus võrgu halvamiseks selle liikmete ründamine ning füüsiline hävitamine. Selleks võib kasutada väga primitiivseid tööriistu, lõhkeainet või elektroonikakomponente lühistavaid elektromagnetrelvi. Praegu masstootmises olevad kübemed on üpriski õrnad ning kaitsetud selliste rünnakute vastu, kuid kui vaadelda seadmeid, mis võiksid kunagi jõuda lahinguväljale, siis on lugu hoopis teine. Kui kübeme näol on tegemist liivatera suuruse objektiga ning neid on lahinguväljale heidetud miljoneid, siis võib arvata, et nende ükshaaval hävitamine ei ole mõeldav ning ka pommitamise efektiivsus ei ole väga kõrge, kuna plahvatustega lihtsalt pillutaks tarka tolmu ühest kohast teise. Selgub ka, et kuna tavapäraste tuumarelvade poolt tekitatava elektromagnetkiirguse lainepikkus on väga pikk, siis ei ole raske luua kübemeid, mis suudaksid seda taluda. Kindlasti on aga võimalik luua spetsiifilisemaid relvi just kübemete hävitamiseks. Natuke teine on lugu teiste võrkudega ühendust võimaldavate seadmetega, kuna üle pikema distantsi sidepidamist võimaldavad seadmed peavad paraku olema mõnevõrra suuremad ning seega ka haavatavamad.

Sensorvõrgu halvamiseks ei pea aga püsivalt hävitama piisavas koguses kübemeid, vaid võib rünnata hoopis ühendusi kübemete vahel. Raadiomoodulite puhul on lihtne häirida kasutatavat

sagedusriba, samas, nagu eelnevalt mainitud, saab sellise rünnaku vastu võidelda laserkommunikatsiooniga. Teatud olukorras võib lihtsalt segajatest efektiivsemaks osutuda aga DDoS tüüpi rünnakud, mille korral kübemed peavad vastuvõetud bitte ka töötlema ning halvemal juhul peavad neid veel vajalikuks edasi saata.

Kuna sensorvõrgus peab turvalisuse tagamiseks kübemete vahel olema teatav usaldus, siis ilmselgelt on need usaldussuhted üheks sihtmärgiks, millele ründajad võivad keskenduda. Ühest küljest peab ründaja saavutama võrgu usalduse selleks, et lugeda või mõjutada seal liikuvaid andmeid. See võib lihtsa vaevaga edukaks osutuda kübemevõrgu esimestel elumomentidel, kus usaldussidemed ei ole veel paigas ja alles selgitatakse välja kasulikke interaktsioone. Teisest küljest on aga võimalik tõsiselt häirida võrgu tööd, kui õnnestub piisavas koguses kübemeid muuta võrgu silmis ebausaldusväärseks. Kui usaldatavate kübemete hulk väheneb, siis muutub väga raskeks toimivate marsruutide leidmine ja informatsiooni liigutamine võrgus. Samuti võib puudulikuks jääda ettekujutus jälgitavast keskkonnast.

Targa tolmu peamiseks eesmärgiks on keskkonnast informatsiooni kogumine erinevate sensorite abil. Kasutatavate sensorite näol on tegemist aga jällegi ühe aspektiga, mida saab rünnata. Osaliselt kübemevõrgus ja osaliselt lõpptarbija juures toimub andmete analüüs, mille käigus filtreeritakse välja vigased mõõtetulemused ning hinnatakse kübemete töökorda. Andmete sorteerimine toimub tavaliselt nende omavahelise sobivuse ja seoste alusel. Potentsiaalselt on aga jälgitavas keskkonnas võimalik tekitada häiringuid, mis muudavad andurite lugemeid ning kas siis täielikult rikuvad ettekujutuse keskkonnatingimustest või tekitavad piisavalt segadust, et sensorvõrgu kasutajad ei saa enam kindlad olla reaalselt toimuvas. Tagajärjeks võib olla segadus lahinguväljal või paanika tsiviilelanikkonna seas, kui näiteks sensorid teavitavad kohesest pilvelõhkuja kokkuvarisemise ohust.

Kaudselt võib ründe alla sattuda ja probleeme tekitada ka kübemetele kõige väärtuslikumat ressurssi pakkuv energiaallikas. Teadagi töötavad kübemed vahelduvate energiatarbe režiimidega, ärgates harva ning säästes ülejäänud aja energiat. Ründajal võib olla aga võimalik tekitada võrgus selline olukord, kus kübemetel ei teki võimalust unerežiimi minna ning energiaallikast jätkub seetõttu vaid väga lühikeseks ajaks. Selline olukord võib tegelikult tekkida ka iseenesest, tingituna kübemevõrgu ilmnevast käitumisest, mida insenerid ei olnud disainifaasis võimelised ette nägema ja testimine välja ei toonud.

Kokkuvõte

Targa tolmu võrgud lubavad realiseerida mitmeid vägagi kasulikke ja huvitavaid lahendusi erinevates eluvaldkondades. Paraku kaasneb kübemete rakendamisega igapäevases keskkonnas mitmeid riske, mille vastu võitlemine ei pruugi olla kuigi lihtne ja ühene ülesanne. Nagu ikka, kehtib siingi põhimõte, et ei ole olemas lukku, mida murda ei saaks – lihtsalt võimalikult keeruliseks tuleb see murdmine teha. Kübemevõrkudel on lisaks ka potentsiaali tulevikus leida kirjeldatud probleemide vastu abi tehisintellekti algetest ja situatsioonitundlikkusest, mis suudaks kokku viia ja rakendada informatsiooni anduritelt, asukohta ruumis, käitumismustreid ja erinevate meetoditega loodud usaldussidemeid.

Kasutatud kirjandus

1. Karlof, C., Sastry, N., Wagner, D. TinySec User Manual, 2004
2. NCSU Cyber Defense Laboratory, TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks. [WWW] http://discovery.csc.ncsu.edu/software/TinyECC/ (06.11.2008)
3. Pister, K. Autonomous sensing and communication in a cubic millimeter. [WWW] http://robotics.eecs.berkeley.edu/~pister/SmartDust/ (06.11.2008)
4. Preden, J. (2006) Communication Area Based Positioning. Mobile Adhoc and Sensor Systems (MASS), 2006 IEEE International Conference on Volume , oktoober 2006 lk 336 - 347